Mannesmann VDO AG

Kruppstraße 105
60388 Frankfurt
4326

Express Mail mailing label
No. EJ450234239US
Deposited August 22, 2000

~~Description~~

Security device

FIELD AND BACKGROUND OF THE INVENTION

The invention relates to a device for actuating a security device, preferably for securing a motor vehicle against unauthorized use, in which a control unit has means for transmitting a first coded electromagnetic signal (stimulus signal), in which a portable transmitter (radio key) has means for receiving the stimulus signal and for transmitting a second coded signal (enable signal), and in which the control unit is connected to the security device and actuates the latter if the enable signal is received and recognized.

Such radio keys are used today for unlocking the doors of motor vehicles without contact, for example. They are known from WO 92/18732, for example.

If the steady-state transmission and reception frequencies for such conventional systems are known, relatively simple transceivers can also forward the stimulus signal over relatively long distances from the vehicle to the authorized user and hence stimulate a key. If appropriate transmitters and receivers are also used for transmitting back the response signal, the response signal can also be traced back to the vehicle and used for unauthorized access to the vehicle.

SUMMARY OF THE INVENTION

The object of the present invention is to ~~specify~~ provide a device for conveniently and contactlessly actuating security devices, in particular the central locking system and immobilizer in motor vehicles, which makes such unauthorized access virtually impossible.

The invention achieves this object ~~by virtue of the feature that~~ wherein both the control unit and the radio key have means for altering the carrier frequency of

the coded electromagnetic signals and that they alter this frequency during signal transmission in a manner which is known only to the control unit and to the radio key. On account of the only very short total transmission time, changing the carrier frequency makes it virtually impossible to monitor the signals and misuse them for unauthorized opening of the security device.

In a first refinement of the invention, the radio key has a narrowband transmitter whose transmission frequency can be controlled, and the radio key alters its transmission frequency over intervals of time when transmitting signals. In addition, the control unit has a tunable narrowband receiver having the same frequency range as the transmitter in the radio key.

In a further refinement of the invention, the manner in which the carrier frequency is to be changed is contained in the stimulus signal as a coded information item for transmission to the radio key.

In this context, provision may be made for the stimulus signal to contain a random number and for the carrier frequencies to be determined by applying a cryptoalgorithm to this stimulus signal and, in this context, particularly to the random number contained in the stimulus signal.

In order to ensure that both the radio key and the control unit change over rapidly to the next carrier frequency in each case, a next refinement of the invention provides for the carrier frequency selection at the receiver and transmitter ends to be determined, using the coded information item in the stimulus signal, by means of a cryptographic method in the radio key and in the control unit independently of one another. Since the necessary information item is produced at both ends in parallel, there is no need for this information item to be transmitted between the control unit and the radio key.

As a basis for generating the separate carrier frequencies for this frequency hopping, the same cryptoalgorithm can be used as for normal message authentication. In this context, the authentication component of the enable signal is at the same time the basis for selection of the discrete carrier frequencies. This has the advantage that no additional computation time need be taken up for generating this data.

In a further refinement of the invention, the signal transmission takes place over a spectrum of different carrier frequencies and the enable signal contains a coded information item for modulating this spectrum. The use of this spread spectrum transmission likewise makes signal transmission very secure.

In this context, the authentication component (for example) of the enable signal can be used as a basis for producing the spread spectrum modulation sequence. In this case, all advantages in terms of computation time taken up etc. are retained. The fact that the present and further spectral distribution of the transmitted signal is known at the transmission and reception ends means that, additionally, the otherwise necessary synchronization or locking on between the transmitter and the receiver is eliminated in the spread spectrum method.

BRIEF DESCRIPTION OF THE DRAWING

Illustrative embodiments of the invention are shown in the drawing with the aid of a plurality of figures and are explained in more detail in the description below. In the figures:

Figure 1 shows a schematic diagram for deriving transmission channels from a stimulus signal, and

Figure 2 shows graphs of the resultant transmission spectra.

In the figures, identical parts are provided with identical reference symbols.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 shows how a radio key uses the stimulus signal 1 (challenge signal) transmitted by the

control unit to determine the sequence of transmission channels n which are to be used and are known at both ends for transmitting signals.

To this end, the stimulus signal 1 is loaded into a ring buffer and is passed through a cryptoalgorithm 3 in steps. The cryptoalgorithm 3 forwards the data stream, comprising bits, in the stimulus signal 1 after a particular volume of data or after a particular time t and thus generates as the result the transmission channel which is to be used for the next transmission sequence. The same procedure also takes place in parallel in the control unit, but in this unit the next reception channels in each case are determined as the result.

The rapid, narrowband changeover cycle, which cannot be anticipated by outsiders, for the carrier frequency makes it impossible to use a single relay radio link to gain unauthorized access to a vehicle.

Figure 2 shows the resultant transmission spectra (A=amplitude) for the radio key when its enable signal is transmitted. Whenever a particular time t or a particular number of data bits has passed, there is a changeover to another channel on the basis of the previously determined sequence. The control unit likewise changes over its reception device synchronously, so that rapid data transmission is assured.